Journal of
CRYPTOLOGY
Volume 10, 1997

The Journal of the International Association for Cryptologic Research

Editor-in-Chief
Gilles Brassard
Département IRO
Université de Montréal
C.P. 6128, succursale centre-ville
Montréal, Québec
Canada H3C 3J7
brassard@iro.umontreal.ca

Editor-in-Chief
Joan Feigenbaum
AT&T Labs Research
Room C203
180 Park Avenue
Florham Park, NJ 07932-0971, USA
jf@research.att.com

Editorial Board

Thomas A. Berson
Anagram Laboratories
764 Forest Avenue
Palo Alto, CA 94301, USA
berson@anagram.com

Ernest F. Brickell
9308 Avenida de la Luna, NE
Albuquerque, NM 87111, USA
brickell@btec.com

Johannes Buchmann
Fachbereich Informatik
Technische Universität Darmstadt
Alexanderstrasse 10
D-64283 Darmstadt, Germany
buchmann@cdc.informatik.th-darmstadt.de

David Chaum
Cryptography Group
Centre for Mathematics and Computer Science
Kruislaan 413
1098 SJ Amsterdam
The Netherlands

Don Coppersmith
IBM Research
Thomas J. Watson Research Center
Yorktown Heights
NY 10598, USA
dcopper@us.ibm.com

Ivan B. Damgård
Matematisk Institut
Aarhus University
Ny Munkegade 116
DK-8000 Aarhus C, Denmark
ivan@daimi.aau.dk

Oded Goldreich
Department of Applied Mathematics and Computer Science
Weizmann Institute of Science
Rehovot 76100, Israel
oded@wisdom.weizmann.ac.il

David Kahn
120 Wooleys Lane
Great Neck, NY 11023, USA

Ueli M. Maurer
Institute for Theoretical Computer Science
ETH Zürich
CH-8092 Zürich, Switzerland
maurer@inf.ethz.ch

Moni Naor
Room 248, Ziskind
Department of Applied Mathematics and Computer Science
Weizmann Institute of Science
Rehovot 76100, Israel
naor@wisdom.weizmann.ac.il

Andrew M. Odlyzko
AT&T Labs Research
Room C225
180 Park Avenue, Building 103
P.O. Box 971
Florham Park, NJ 07932-0971, USA
amo@research.att.com

Bart Preneel
Department of Electrical Engineering
Katholieke Universiteit Leuven
Kardinaal Mercierlaan 94
B-3001 Heverlee, Belgium
bart.preneel@esat.kuleuven.ac.be

Steven Rudich
School of Computer Science
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213-3890, USA
rudich@theory.cs.cmu.edu

Othmar Staffelbach
UG FU Sektion Kryptologie
Hofweg 11
CH-3003 Bern, Switzerland
staffel@inf.ethz.ch

Jacques Stern
Département de mathématiques
École Normale Supérieure
45 rue d'Ulm
75230 Paris cedex 05, France
Jacques.Stern@ens.fr

Aims and Scope

Journal of Cryptology provides a forum for original results in all areas of modern information security. Both cryptography and cryptanalysis are covered, including information theoretic and complexity theoretic perspectives as well as implementation, application, and standards issues. Illustrative topics include public key and conventional algorithms and their implementations, cryptanalytic attacks, pseudo-random sequences, computational number theory, cryptographic protocols, untraceability, privacy, authentication, key management, and quantum cryptography. In addition to full-length technical, survey, and historical articles, short notes are acceptable.

The exclusive copyright for all languages and countries, including the right for photomechanical and any other reproductions, also in microform, is transferred to the publisher.
The use of registered names, trademarks, etc., in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Printed in the United States of America
© 1997 International Association for Cryptologic Research

Index to Volume 10

BEAVER, D.: Locally Random Reductions: Improvements and Applications .. 17
BELLER, M. J.: *see* YACOBI, Y. 89
BIHAM, E.: An Improvement of Davies' Attack on DES 195
BIRYUKOV, A.: *see* BIHAM, E. 195
CACHIN, C.: Linking Information Reconciliation and Privacy Amplification 97
COPPERSMITH, D.: Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities 233
COPPERSMITH, D.: The Security of the Birational Permutation Signature Schemes 207
CSIRMAZ, L.: The Size of a Share Must Be Large 223
DAMGÅRD, I. B.: On the Existence of Statistically Hiding Bit Commitment Schemes and Fail-Stop Signatures 163
DOBBERTIN, H.: RIPEMD with Two-Round Compress Function Is Not Collision-Free 51
EVEN, S.: A Construction of a Cipher from a Single Pseudorandom Permutation 151
FEIGENBAUM, J.: *see* BEAVER, D. 17
FIAT, A.: Batch RSA 75
GORESKY, M.: *see* KLAPPER, A. 111
HIROKI SHIZUYA: *see* TOSHIYA ITOH 37
JACKSON, W.-A.: Mutually Trusted Authority-Free Secret Sharing Schemes 261
KALISKI, B. S., JR.: A Chosen Message Attack on Demytko's Elliptic Curve Cryptosystem 71
KILIAN, J.: *see* BEAVER, D. 17
KLAPPER, A.: Feedback Shift Registers, 2-Adic Span, and Combiners with Memory 111
MANSOUR, Y.: *see* EVEN, S. 151
MARTIN, K. M.: *see* JACKSON, W.-A. 261
MAURER, U. M.: *see* CACHIN, C. 97
O'KEEFE, C. M.: *see* JACKSON, W.-A. 261
PEDERSEN, T. P.: *see* DAMGÅRD, I. B. 163
PFITZMANN, B.: *see* DAMGÅRD, I. B. 163
ROGAWAY, P.: *see* BEAVER, D. 17
DE ROOIJ, P.: On Schnorr's Preprocessing for Digital Signature Schemes 1
STERN, J.: *see* COPPERSMITH, D. 207
TOSHIYA ITOH: A Language-Dependent Cryptographic Primitive 37
VAUDENAY, S.: *see* COPPERSMITH, D. 207
YACOBI, Y.: Batch Diffie–Hellman Key Agreement Systems 89
YUJI OHTA: *see* TOSHIYA ITOH 37